REMARKS

Claims 21-45 and 48 are pending in the case. The Examiner rejected all of the claims over cited prior art. Independent claim 21 has been amended. The following remarks are considered by applicant to overcome each of the Examiner's outstanding rejections. An early Notice of Allowance therefore requested.

The Examiner rejected claims 21-31, 33-36, 38, 40, 41, 44, 45 and 47 under 35 USC 102 and being anticipated by Rai (US 6,377,982). The Examiner also rejected claims 32, 37, 39, 42 and 43 under 35 USC 103 as being unpatentable over Rai. In rejecting claim 21 as being anticipated by Rai, the Examiner contends that Rai describes the invented system as recited in claim 21. Applicant has amended claim 21 to clarify the nature of the invention. In particular, this claim has been amended to detail the authentication process in the present invention.

Rai describes the registration process and authentication process for a roaming end system in col. 18, line 16- col. 19, line 67 and in fig. 14. In that process, the end system sends a request to the foreign agent in a foreign network. Col. 18, lines 37-41. The foreign agent sends that request to the foreign registration server and the foreign registration server forwards a registration request to the home registration server. Lines 42-44 and lines 51-55. The home server then authenticates the foreign service provider. Lines 55-58. After that authentication process, the home registration server begins the process of setting up a communication path through IWFs between the home server and the foreign server. Col. 18, lines 61 – col. 19, line 7. This setup of the communication path occurs only after the foreign server is authenticated to the home server. This is necessary because (1) the home server must verify that the there exists an agreement between the home server and the foreign server as part of a security measure and (2) an accounting must be established as between the home server and the foreign server. Such an authentication step reflects the lack of trust that existed in prior art systems.

This is different from the currently claimed system. The host system has been configured to direct all communication to the CTA that resides on the host system. The CTA is a trusted piece of software that resides on the host system. The client system will communicate with the CTA residing on the host system and all communication will be through the CTA. As such, there is no authentication process necessary as between the host system and the target system as the concerns that would require authentication are not present. The security concerns

that are present in the prior art systems are not present in the present invention. Since all communication between the host system and the target system will be limited to the CTA, none of the resources of the host system will be involved; thereby eliminating security concerns on behalf of the host system. Any security concerns of the host system were dealt with when the CTA was placed on the host system and not at the time of access by a client system.

Similarly, there are no security concerns on the target system's side about authenticating the host system since it is the CTA that is communicating with the target system. The CTA is a trusted piece of software that is placed on the host systems by a pre-arranged agreement. Moreover, the client system will still need to be authenticated by the target system before access to the target system is allowed.

Additionally, the same accounting issues are not raised because of a change of mindset regarding revenue generation. In prior art systems, each company was very territorial and keeping track of user and access points was key to revenue. In the present invention, this revenue generation is of less concern. The target system does not care whether or not the host system is authentic because increased coverage is more beneficial to the target system. If an inauthentic host system were to attempt to access the target system on behalf of a legitimate client system, then that results in a positive result for the target network. The vetting that occurs by the presence of the CTA on the host system and the authentication of the client system to the target system provides the sufficient level of security. Hence, the authentication of the host system to the target system is rendered unnecessary.

Thus, Rai does not describe amended claim 21 which recites "a step of connecting the client system to the target network via a host system controlled by the software provided in the client system *without needing to authenticate said host system to said target system*" (emphasis added). As such, claim 21 is allowable.

Claims 22-45 and 48 are dependent claims on claim 21 and should be allowable for the same reasons that claim 21 is allowable.

In view of the foregoing, it is respectfully submitted that the claims are in condition for allowance and favorable reconsideration and prompt notice to that affect are earnestly solicited.

Respectfully submitted,

Date: September 30, 2010

Stephen M. Chin
Reg. No. 39,938
Attorney For Applicants
von Simson & Chin LLP
62 William Street – Sixth Floor
New York, New York 10005
ph (212) 514-8645
direct dial (212) 514-8653
fax (212) 514-8648
smc@vsandc.com